

iSekurity Frequently Asked Questions

How our service works:

1. What does iSekurity service provide?

When you become a member of iSekurity we take a proactive position by immediately initiating our proprietary Sekure ScanSM to create your comprehensive “life history” report to detect any suspicious activity early. Within 90 days of enrolling, you will receive an email confirming that your Sekure ScanSM report is ready for review via our secure, members-only website.

Secondly, if you become a victim, we assist you in the immediate credit restoration process and provide insurance through a 3rd party insurer to cover your restoration costs up to \$25,000.

Most importantly, we are the only ID theft protection provider that will aggressively investigate the crime against you. We initiate an investigation to identify and locate the party responsible for the crime against you and assist in arrest and prosecution. Stopping criminals in their tracks is the only effective means of truly combating identity theft.

2. Do I have to do anything else after signing up?

Once you receive your new member ID via email, please login to the website

(www.isekurity.com) to visit your private member page using your member ID and password.

Within 90 days of enrolling, you will receive an email notifying you that your **SeKure ScanSM** is available for your review on our secure, members-only website. You do not have to do anything further once you have signed up. We encourage you to visit the web site periodically to review informative news postings and useful tips for members.

3. What will I receive once I enroll in iSekurity?

- First, you will receive an email with your member ID. You can login to our website (www.isekurity.com) using your member ID and password to have access to the members-only area. This exclusive, members-only area will allow you to access your account, personal information, and the latest news on iSekurity.
- Second, you will receive a welcome letter in the mail 7-10 days after your enrollment with iSekurity with your wallet membership ID card. The card will have your name, member ID, and important iSekurity contact numbers for your easy reference. In addition, there is a warning on the back of the card to ID thieves that you are protected by a team of former federal agents and any theft or fraudulent use of your personal information will be aggressively investigated.
- With iSekurity Premium Plans, you will have access to your initial SeKure ScanSM results within 90 days from your enrollment date. This proprietary multiple databases creates your comprehensive “life history” report to help detect suspicious activity early. You will be able to access and review the scan results on our website in the secure, members-only-service section.

4. When will I be contacted for additional information?

You will not be contacted by iSecurity for additional information in normal circumstances. The circumstances that would require us to contact you for additional information would be if your SeKure ScanSM results indicate a potential threat against you or if you have become a victim and we have initiated an investigation.

5. What is a SeKure ScanSM?

The SeKure ScanSM is iSecurity's proprietary technology initiated once you enroll to create your comprehensive "life history" report which includes everything from your entire address history and all registered financial account information to criminal acts committed in your name. The SeKure ScanSM process is a comprehensive search of multiple data sources in an effort to detect any breach or potential threat early. The system combines the best of iSecurity's technology and agent expertise to make a thorough assessment on your behalf.

6. Can I decline the SeKure ScanSM?

Yes. This is a personal choice for the members but we encourage the scan as a preventative measure.

7. What type of data sources are checked for SeKure ScanSM?

The data sources checked for SeKure ScanSM are proprietary and only our team of iSecurity experts have access to them. The scan reports everything from your entire address history and all registered financial account information to criminal acts committed in your name and weapons registered in your name as well.

8. How far back does SeKure ScanSM look?

Your entire life will be included in the SeKure ScanSM report. You will receive a new SeKure ScanSM annually, while you are a iSecurity member.

9. Does SeKure ScanSM pick up real estate overseas?

Yes.

10. What are my responsibilities after my identity is stolen as a member of iSecurity?

As an iSecurity member, you need only call our 24/7 Victim Hotline and we will guide you through the recovery process.

In short, immediate first steps for you to take include the following 3 actions:

- We will instruct you to immediately file a police report and complete the iSecurity affidavit and return it to us so we can start the criminal investigation.
- We will instruct you to notify your credit card providers and banks to stop payment.
- We will instruct you on how to set fraud alerts on your account with the 3 credit bureaus.

Our Command Center representatives will guide you through the initial process of obtaining a police report and faxing it to us. You will also be required to provide a notarized affidavit. Our representatives will instruct you on how to download and print the affidavit form from our website. We will need to have both the police report and notarized affidavit in our possession in order to begin the investigation. Once we have both of the forms we will assign you a case manager from our team of former Federal Agents and initiate the investigation of the crime. Your case manager will keep you informed throughout the course of the investigation. Our Command Center will assist you with everything required to restore your credit. We will work with you for reimbursement of your expenses through our 3rd party insurer's policy.

11. How will you help restore immediate good credit?

We will advise you throughout the Recovery process our Command Center Representatives, along with the Fraud Restoration Specialist (from our 3rd party insurer) will assist with all administrative activities. Case Manager (former Federal agent) will provide you a case report that details the incidents to use to expedite your credit restoration.

The detailed investigative report will be used to provide to the credit bureaus and any other financial institutions showing the evidence and facts of your case. This report is signed and duly authorized by your Case Manager (Former Federal Agent) attesting to its validity.

12. Do you do credit monitoring or set fraud alerts?

No, we do not do credit monitoring or set fraud alerts. However, iSekurity supports these types of preventive measures recommended by the FTC when utilized properly. These services were established for you to do yourself for free! If you notice any suspicious activity in your account, you can easily contact the credit bureaus toll-free or via their websites to set a fraud alert. These alerts will let potential creditors know that you may be a victim of identity theft. Please visit the prevention section of our web site (www.isekurity.com) for simple instructions on how to set a fraud alert. We advise members that credit monitoring and fraud alerts are a limited means of prevention. No matter what detection and/or deterrents you have in place there is nothing out there that can protect you 100% against identity theft.

13. What if I enroll with iSekurity and didn't realize that I was already a victim of identity theft – will you, iSekurity, still cover me and pursue the investigation?

This situation will be handled on a case by case basis.

14. If you do not monitor my credit or set fraud alerts, how are you helping to protect my identity?

We help protect your identity by initiating our proactive Sekure Scan process and by going to the root cause of the breach and attempting to neutralize it. We know that no matter how many deterrent and detection services you use nothing is full proof. When someone steals your identity you need to find out who did it and stop them from doing it again. The Secret Service statistics on ID theft crime show an ID theft criminal uses your identity an average of 30 times. They are able to do this because no one is going after the criminal. By becoming a member of iSekurity, you will be affiliated with the nation's largest team of former Federal Agents dedicated to fighting identity theft.

15. Will I have to do anything...or, will my assigned Case Manager handle the whole investigation?

Our expert agents will manage your case and handle all aspects of the investigation. To manage the investigation, our agents may need you to provide details to assist them in closing the case.

16. What does the \$25,000 insurance cover?

The insurance covers loss resulting from an identity theft and provides the member restoration services after an identity theft. This insurance coverage is provided by a third party insurance provider.

17. What type of loss is covered?

The insurance covers loss resulting from an identity theft including costs, loss wages and legal fees. This insurance coverage is provided by a third party insurance provider. You will be reimbursed for up to \$25,000 per year, with no deductible, for restoration costs, loss wages and legal fees incurred associated with identity theft, such as:

- **COSTS**
 - Costs incurred for re-filing applications for loans, grants, or other credit instruments that were rejected because of the identity theft.
 - Costs to report and/or amend identity theft such as
 - Notarizing affidavits
 - Long distance telephone calls
 - Postage
 - Costs for up to 6 credit reports
- **LOST WAGES** earned in the US (Maximum \$500 per week/ max 4 weeks)
 - For time taken off work to amend or rectify records as to the member's true name and identity. Examples may include time to meet with law enforcement agencies, credit agencies, financial institutions, credit agencies and/or legal counsel;
 - for time taken off to resolve an identity theft issue
- **LEGAL DEFENSE FEES AND EXPENSES**
 - Defense of civil lawsuits brought against victim
 - Removal of civil judgments wrongly entered against victim because of identity theft

18. What is included in the restoration services?

Members will be provided a general packet of information about the financial reimbursement process; you will be assigned a Fraud Restoration Specialist to guide you through recovery, along with a Case Manager (Former Federal Agent) to manage the investigation.

19. Does my policy cover lost wages if I have to take time off work to fix my credit?

Yes. The policy covers actual lost wages that would have been earned in the US, for time taken off work and away from work premises to amend and/or rectify records as to member's true name and identity. The limit to the policy is \$500 per week and 4 weeks maximum. Time taken from self employment is not covered.

20. Does my policy cover my spouse and children as well?

No. Under this policy only the natural person on record with the insurance provider is covered.

21. What should I do if I am a victim of identity theft and I am a member of iSekurity?

If you believe your identity has been compromised and you are an iSekurity member, login to your member page at www.iSekurity.com to access our Victim Hotline. If you cannot login, you can speak with someone at the Command Center by calling 1-877-838-5734 (toll-free). Please have your iSekurity Member ID number available.

22. What should I do if a loss occurs as a result of the identity theft?

Promptly contact the Command Center for immediate assistance at 1-877-838-5734.

23. Why don't we have a \$1 Million Service Guarantee like some providers?

We actually carry a \$2 Million Limit of Liability - the reason we don't advertise this is because we feel it misleads our customers. Other companies call it a service guarantee making it appear as though if you have your identity stolen...you get \$1 million. That is not true. The service guarantee or limit of liability only protects the company from gross negligence. Any losses you incur from gross negligence on behalf of the company protecting you will be covered.

24. Will I have direct contact with the Federal Agent that handles my case? Yes. You will be working closely with the agent throughout the investigative process.

25. What happens to the criminals once they are caught? We do our best to utilize our relationships within Federal, State and local government to have them arrested and prosecuted.

26. Why do I care if you ever catch the person who did this to me?

Secret Service statistics show on average a criminal will use your identity 30 times. The only way you can prevent this is by catching and stopping the criminal in their tracks.

27. Will iSekurity take the case to the prosecuting attorney?

iSekurity will turn the case over to the proper law enforcement agency once substantial evidence has been gathered against the alleged identity thief. The law enforcement agency then takes the case to the prosecuting attorney. Your iSekurity assigned case manager will continue to monitor the case and report back to you on the details of the prosecution.

28. What if the criminal turns out to be someone in my family or friend who I do not want to be prosecuted? Can I cancel the investigation?

Yes, you can request to stop the investigation. If you do wish to halt the investigation, you will need to sign a statement releasing iSekurity from responsibility.

29. Am I required to give iSekurity my Social Security Number?

No. In normal circumstances iSekurity does not need or ask for you SSN#. We instruct you through our web site NOT to give out your SSN unless you are convinced it is absolutely necessary and you trust the requesting source.

General ID Theft Questions:

30. What is identity theft?

Identity theft occurs when someone uses your personal identifying information, like your name, Social Security number, or to apply for new credit, without your permission, to commit fraud or other crimes.

The FTC estimates that as many as 9 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many hours repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

31. How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when Processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by Completing a change of address form.
5. **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

32. What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways.

Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.
-

Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

33. How can you find out if your identity was stolen?

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. Under federal law, you have the right to receive a free copy of your credit report once every 12 months from each of the nationwide consumer reporting companies. You can order your free annual credit report from www.annualcreditreport.com or call 1-877-322-8228. Stagger your requests from the three bureaus and obtain one report every four months to monitor your information on an ongoing basis.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

34. How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. It depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report. Victims of identity theft should Set Fraud Alerts and monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

35. What can you do to help fight identity theft?

A great deal.

Awareness is an effective weapon against many forms of identity theft. Be aware of how information is stolen and what you can do to protect yourself, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community. The FTC has prepared a collection of easy-to-use materials to enable anyone regardless of existing knowledge about identity theft to inform others about this serious crime.

36. What is a fraud alert?

A fraud alert is a flag that you can have set on your credit report through the 3 consumer reporting agencies. This flag establishes that as part of any credit approval process, you need to be notified prior to new credit being issued. It is intended to be used by consumers who believe they have an identity theft problem. The alert is set for 90 days and then removed unless reset again. Fraud alerts do not prevent an identity thief from co-opting and using one of your credit cards. They also don't prevent someone from using your social security number to work. They further don't prevent thieves from signing up for utilities or telecommunications services using your identity. And they don't stop someone from using your personal information to get access to health care services.

Fraud alerts also do not prevent inquiries for credit from showing up on a victim's credit report. These events can have a negative effect on a person's credit score. Fraud alerts do have their place in dealing with a threat to your financial identity, particularly in some forms of new account fraud but they are not a silver bullet and certainly are not a guarantee that individuals won't fall victim to identity theft.

37. What is a credit freeze?

Many states have laws that let consumers "freeze" their credit – in other words, letting a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. This means that it's unlikely that an identity thief would be able to

open a new account in your name. Placing a credit freeze does not affect your credit score – nor does it keep you from getting your free [annual credit report](#), or from buying your credit report or score.

Credit freeze laws vary from state to state. In some states, anyone can freeze their credit file, while in other states, only identity theft victims can. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, while other consumers pay a fee – typically \$10. It's also important to know that these costs are for each of the credit reporting agencies. If you want to freeze your credit, it would mean placing the freeze with each of three credit reporting agencies, and paying the fee to each one.

38. Who can access my credit report if I place a credit freeze?

If you place a credit freeze, you will continue to have access to your free [annual credit report](#). You'll also be able to buy your credit report and credit score even after placing a credit freeze. Companies that you do business with will still have access to your credit report – for example, your mortgage, credit card, or cell phone company – as would collection agencies that are working for one of those companies. Companies will also still be able to offer you prescreened credit. Those are the credit offers you receive in the mail that you have not applied for. Additionally, in some states, potential employers, insurance companies, landlords, and other non-creditors can still get access to your credit report with a credit freeze in place.

39. Can I temporarily lift my credit freeze if I need to let someone check my credit report?

If you want to apply for a loan or credit card, or otherwise need to give someone access to your credit report and that person is not covered by an exception to the credit freeze law, you would need to temporarily lift the credit freeze. You would do that by using a PIN that each credit reporting agency would send once you placed the credit freeze. In most states, you'd have to pay a fee to lift the credit freeze. [Most states](#) currently give the credit reporting agencies three days to lift the credit freeze. This might keep you from getting "instant" credit, which may be something to weigh when considering a credit freeze.

40. How does a thief use my identity up to 30 times?

Most ID theft cases are never investigated. Thieves still have your information and free reign to do whatever they wish with it. According to Secret Service statistics, 70% of ID thieves do not have a prior criminal record so they keep doing what they're doing until they get caught.

41. Why are college students so vulnerable?

College students are vulnerable for several reasons. One, there are constant promotions by credit card issuers requiring students to fill out credit applications for free promotional gifts. Students complete the forms and throw them out making them an easy target for ID thieves. Additionally, for the most part, college students have clean credit records making them attractive targets. Also, many schools still collect and use a student's social security numbers in their database records.

42. What should I do to protect my social security number?

This is the single most coveted piece of information an identity thief wants to possess. Don't carry your Social Security Card in your wallet or write it on a check; don't share it with your friends, with unproven sources or use it as a gimmick or test. Anytime someone asks for your

Social Security Number, ask them questions: Why do you need it? How will my SSN be used? What law requires me to give you my SSN? What will happen if I don't give you my SSN? Only when these questions are satisfied should you then share this highly sensitive piece of personal data.

43. How should I go about protecting my personal information?

Don't give out personal information on the phone, through the mail, or over the Internet unless you are comfortable with the source.

Keep your personal information in a safe place at home, away from visitors, roommates or outside help working in your home. Find out the information security procedures where you work and at other places that request personal information: such as your doctor's office, educational institutions, etc. Have them verify that your data is handled securely.

44. Should I shred mail and paper documents?

Yes. Shred financial documents and paperwork with personal information before you discard them. Also, in order to cut down on the junk mail, you can remove your name from pre-approved credit card lists and junk mail lists. To opt out of receiving offers of credit or insurance in the mail call 1-888-567-8688. If you are traveling away from home, call the US Postal Service at 1-800-275-8777 to request a vacation hold of your mail until you return.

45. How do I keep myself protected on the internet?

In today's world, the Internet has turned into a very dangerous place. Here are some tips on you to protect yourself on the electronic front.

1. Put protection software in place on your home computers. Use firewalls for your home networks and protect your computer with anti-virus, anti-spyware and anti-fraud protection software. Keep these and your operating systems regularly updated from your technology provider.
2. Use a secure browser that will encrypt information you send out. Look for the "lock" icon in the browser's status bar to assure that your transmissions are secure.
3. Make sure you turn off your computer when not in use. Log off when you are finished with a program.
4. Don't provide your credit card online unless you are making a purchase from a website you trust. Secure sites will direct you to a secure page with a URL starting with https:// whenever you make purchases or are asked to provide confidential information.
5. When transacting online, look for the website merchant's privacy policy. It will tell you about the security and use of your personal data. Reconsider doing business if a privacy policy does not exist or you don't agree with the one provided.
6. Avoid clicking on links sent in unsolicited emails. Don't open emails sent by strangers or download software from a source you don't know.
7. Password protect as much of your personal information as possible and avoid using obvious passwords such as your mother's maiden name, last four digits of your social security number, or your birth date.

8. Delete all personal information from a computer before you dispose of it. It is best to use utility software that wipes out the computer's hard drive.
9. Don't store credit card numbers and other financial data on your cell phone or PDA.

46. Is there anything else I can do to protect myself from Identity Theft?

Monitor your bank and credit card transactions on your statements for unauthorized use. Thieves often begin by trying to make small unnoticed transactions on your account. You are going to want to obtain and inspect your credit reports periodically, and make sure there's no unfamiliar or suspicious activity reflected on the reports. To order your FREE annual report from any of the national credit reporting companies, you can visit www.annualcreditreport.com or call 1-877-322-8228. You can also set a fraud alert on your account with the 3 Credit Reporting Companies. Fraud alerts will help reduce the chance of new account fraud. When your fraud alert is set a business cannot issue credit in your name without contacting you for your approval. You can set these alerts yourself for free through the Credit Report Companies either online or through their toll free number. You only have to set the alert through one of the Credit Reporting Companies and they are required to contact the other two. Their phone numbers and web addresses are below.

1. Equifax: 1-800-525-6285 www.equifax.com
2. Experian: 1-888-397-3742 www.experian.com
3. TransUnion: 1-800-680-7289 www.transunion.com

47. How can I tell if I have become a victim?

If an identity thief is opening credit accounts in your name, these accounts are likely to show up on your credit report. To find out, order a copy of your credit reports. Once you receive your reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check all information, like your social security number; address (es), name or initials, and employers. Be sure they are correct. If you find fraudulent or inaccurate information, get it removed. Continue to check your reports periodically.

Look for additional signs of identity theft such as:

1. Failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his/her tracks
2. Receiving credit cards that you didn't apply for
3. Being denied credit or being offered less favorable credit terms, like a high interest rate, for no apparent reason
4. Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

49. What do I do if I become a victim?

If your identity has been compromised and you are not a member of iSecurity this is what you should do immediately:

1. Contact the three national Credit Reporting Companies and place fraud alerts.
2. Contact your financial institutions and credit card issuers and close the account that you believe has been fraudulently accessed.
3. Send notification letters to your creditors, debt collectors, and law enforcement agencies advising that you are a victim of identity theft.
4. Make an appointment to meet with the appropriate law enforcement agency, as well as organizing your information prior to your appointment.
5. Gather key documents and data related to your identity and accounts
6. Contact the Federal Trade Commission and alert them you are a victim of identity theft: www.ftc.gov.

50. Will the SeKure ScanSM impact my credit report/score?

No, the SeKure ScanSM searches proprietary databases and will not impact your credit score.